



ONTAP network information

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/networking/view_network_information_overview.html on February 12, 2026. Always check docs.netapp.com for the latest.

Table of Contents

ONTAP network information	1
View ONTAP network information	1
View ONTAP network port information	1
View ONTAP VLAN information	3
View ONTAP interface group information	3
View ONTAP LIF information	4
View routing information for the ONTAP network	7
View ONTAP DNS host table entries	9
View ONTAP DNS domain configuration information	9
View ONTAP failover group information	10
View ONTAP LIF failover targets	11
View ONTAP LIFs in a load balancing zone	13
Examples of displaying load balancing zones for LIFs	13
View ONTAP cluster connections	14
Display active connections by client (cluster administrators only)	14
Display active connections by protocol (cluster administrators only)	15
Display active connections by service (cluster administrators only)	16
Display active connections by LIF on a node and SVM	17
Display active connections in a cluster	18
Display listening connections in a cluster	19
ONTAP commands to diagnose network problems	20
View network connectivity with neighbor discovery protocols	21
View ONTAP network connectivity with neighbor discovery protocols	21
Use CDP to detect ONTAP network connectivity	22
Use LLDP to detect ONTAP network connectivity	28

ONTAP network information

View ONTAP network information

Using the CLI, you can view information related to ports, LIFs, routes, failover rules, failover groups, firewall rules, DNS, NIS, and connections. Beginning with ONTAP 9.8, you can also download the data that is displayed in System Manager about your network.

This information can be useful in situations such as reconfiguring networking settings, or when troubleshooting the cluster.

If you are a cluster administrator, you can view all the available networking information. If you are an SVM administrator, you can view only the information related to your assigned SVMs.

In System Manager, when you display information in a *List View*, you can click **Download**, and the list of objects displayed is downloaded.

- The list is downloaded in comma-separated values (CSV) format.
- Only the data in the visible columns is downloaded.
- The CSV filename is formatted with the object name and a time stamp.

View ONTAP network port information

You can display information about a specific port, or about all ports on all nodes in the cluster.

About this task

The following information is displayed:

- Node name
- Port name
- IPspace name
- Broadcast domain name
- Link status (up or down)
- MTU setting
- Port speed setting and operational status (1 gigabit or 10 gigabits per second)
- Auto-negotiation setting (true or false)
- Duplex mode and operational status (half or full)
- The port's interface group, if applicable
- The port's VLAN tag information, if applicable
- The port's health status (health or degraded)
- Reasons for a port being marked as degraded

If data for a field is not available (for example, the operational duplex and speed for an inactive port would not be available), the field value is listed as –.

Step

Display network port information by using the `network port show` command.

You can display detailed information for each port by specifying the `-instance` parameter, or get specific information by specifying field names using the `-fields` parameter.

```
network port show
Node: node1

Ignore
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  degraded
false
e0d      Default      Default      up    1500  auto/1000  degraded
true
Node: node2

Ignore
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  healthy
false
e0d      Default      Default      up    1500  auto/1000  healthy
false
8 entries were displayed.
```

Learn more about `network port show` in the [ONTAP command reference](#).

View ONTAP VLAN information

You can display information about a specific VLAN or about all VLANs in the cluster.

About this task

You can display detailed information for each VLAN by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

Step

Display information about VLANs by using the `network port vlan show` command. The following command displays information about all VLANs in the cluster:

```
network port vlan show
      Network Network
  Node  VLAN Name Port    VLAN ID  MAC Address
----- -----
cluster-1-01
    a0a-10    a0a     10    02:a0:98:06:10:b2
    a0a-20    a0a     20    02:a0:98:06:10:b2
    a0a-30    a0a     30    02:a0:98:06:10:b2
    a0a-40    a0a     40    02:a0:98:06:10:b2
    a0a-50    a0a     50    02:a0:98:06:10:b2
cluster-1-02
    a0a-10    a0a     10    02:a0:98:06:10:ca
    a0a-20    a0a     20    02:a0:98:06:10:ca
    a0a-30    a0a     30    02:a0:98:06:10:ca
    a0a-40    a0a     40    02:a0:98:06:10:ca
    a0a-50    a0a     50    02:a0:98:06:10:ca
```

Learn more about `network port vlan show` in the [ONTAP command reference](#).

View ONTAP interface group information

You can display information about an interface group to determine its configuration.

About this task

The following information is displayed:

- Node on which the interface group is located
- List of network ports that are included in the interface group
- Interface group's name
- Distribution function (MAC, IP, port, or sequential)
- Interface group's Media Access Control (MAC) address
- Port activity status; that is, whether all aggregated ports are active (full participation), whether some are active (partial participation), or whether none are active

Step

Display information about interface groups by using the `network port ifgrp show` command.

You can display detailed information for each node by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

The following command displays information about all interface groups in the cluster:

```
network port ifgrp show
  Port      Distribution
  Node     IfGrp     Function      MAC Address      Active
-----  -----  -----  -----  -----  -----
cluster-1-01
  a0a      ip          02:a0:98:06:10:b2  full      e7a, e7b
cluster-1-02
  a0a      sequential   02:a0:98:06:10:ca  full      e7a, e7b
cluster-1-03
  a0a      port         02:a0:98:08:5b:66  full      e7a, e7b
cluster-1-04
  a0a      mac          02:a0:98:08:61:4e  full      e7a, e7b
```

The following command displays detailed interface group information for a single node:

```
network port ifgrp show -instance -node cluster-1-01

  Node: cluster-1-01
  Interface Group Name: a0a
  Distribution Function: ip
    Create Policy: multimode
    MAC Address: 02:a0:98:06:10:b2
  Port Participation: full
    Network Ports: e7a, e7b
    Up Ports: e7a, e7b
    Down Ports: -
```

Learn more about `network port ifgrp show` in the [ONTAP command reference](#).

View ONTAP LIF information

You can view detailed information about a LIF to determine its configuration.

You might also want to view this information to diagnose basic LIF problems, such as checking for duplicate IP addresses or verifying whether the network port belongs to the correct subnet. storage virtual machine (SVM) administrators can view only the information about the LIFs associated with the SVM.

About this task

The following information is displayed:

- IP address associated with the LIF
- Administrative status of the LIF
- Operational status of the LIF

The operational status of data LIFs is determined by the status of the SVM with which the data LIFs are associated. When the SVM is stopped, the operational status of the LIF changes to down. When the SVM is started again, the operational status changes to up

- Node and the port on which the LIF resides

If data for a field is not available (for example, if there is no extended status information), the field value is listed as -.

Step

Display LIF information by using the `network interface show` command.

You can view detailed information for each LIF by specifying the `-instance` parameter, or get specific information by specifying field names using the `-fields` parameter.

The following command displays general information about all LIFs in a cluster:

```

network interface show
  Logical      Status      Network      Current      Current  Is
Vserver      Interface  Admin/Oper  Address/Mask  Node       Port
Home

-----
-----
example
  lif1        up/up      192.0.2.129/22  node-01
                                         e0d
false
node
  cluster_mgmt up/up      192.0.2.3/20   node-02
                                         e0c
false
node-01
  clus1       up/up      192.0.2.65/18  node-01
                                         e0a
true
  clus2       up/up      192.0.2.66/18  node-01
                                         e0b
true
  mgmt1      up/up      192.0.2.1/20   node-01
                                         e0c
true
node-02
  clus1       up/up      192.0.2.67/18  node-02
                                         e0a
true
  clus2       up/up      192.0.2.68/18  node-02
                                         e0b
true
  mgmt2      up/up      192.0.2.2/20   node-02
                                         e0d
true
vs1
  d1          up/up      192.0.2.130/21  node-01
                                         e0d
false
  d2          up/up      192.0.2.131/21  node-01
                                         e0d
true
  data3       up/up      192.0.2.132/20  node-02
                                         e0c
true

```

The following command shows detailed information about a single LIF:

```
network interface show -lif data1 -instance

          Vserver Name: vs1
          Logical Interface Name: data1
          Role: data
          Data Protocol: nfs,cifs
          Home Node: node-01
          Home Port: e0c
          Current Node: node-03
          Current Port: e0c
          Operational Status: up
          Extended Status: -
          Is Home: false
          Network Address: 192.0.2.128
          Netmask: 255.255.192.0
          Bits in the Netmask: 18
          IPv4 Link Local: -
          Subnet Name: -
          Administrative Status: up
          Failover Policy: local-only
          Firewall Policy: data
          Auto Revert: false
          Fully Qualified DNS Zone Name: xxx.example.com
          DNS Query Listen Enable: false
          Failover Group Name: Default
          FCP WWPN: -
          Address family: ipv4
          Comment: -
          IPspace of LIF: Default
```

Learn more about `network interface show` in the [ONTAP command reference](#).

View routing information for the ONTAP network

You can display information about routes within an SVM.

Step

Depending on the type of routing information that you want to view, enter the applicable command:

To view information about...	Enter...
Static routes, per SVM	<code>network route show</code>

LIFs on each route, per SVM

```
network route show-lifs
```

You can display detailed information for each route by specifying the `-instance` parameter. The following command displays the static routes within the SVMs in cluster-1:

```
network route show
Vserver          Destination      Gateway      Metric
-----
Cluster
          0.0.0.0/0      10.63.0.1      10
cluster-1
          0.0.0.0/0      198.51.9.1      10
vs1
          0.0.0.0/0      192.0.2.1      20
vs3
          0.0.0.0/0      192.0.2.1      20
```

The following command displays the association of static routes and logical interfaces (LIFs) within all SVMs in cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination      Gateway      Logical Interfaces
-----
0.0.0.0/0      10.63.0.1      -
Vserver: cluster-1
Destination      Gateway      Logical Interfaces
-----
0.0.0.0/0      198.51.9.1      cluster_mgmt,
                                         cluster-1_mgmt1,
Vserver: vs1
Destination      Gateway      Logical Interfaces
-----
0.0.0.0/0      192.0.2.1      data1_1, data1_2
Vserver: vs3
Destination      Gateway      Logical Interfaces
-----
0.0.0.0/0      192.0.2.1      data2_1, data2_2
```

Learn more about `network route show` and `network route show-lifs` in the [ONTAP command reference](#).

View ONTAP DNS host table entries

The DNS host table entries map host names to IP addresses. You can display the host names and alias names and the IP address that they map to for all SVMs in a cluster.

Step

Display the host name entries for all SVMs by using the vserver services name-service dns hosts show command.

The following example displays the host table entries:

```
vserver services name-service dns hosts show
Vserver      Address          Hostname       Aliases
-----
cluster-1
          10.72.219.36    lnx219-36      -
vs1
          10.72.219.37    lnx219-37      lnx219-37.example.com
```

You can use the vserver services name-service dns command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

View ONTAP DNS domain configuration information

You can display the DNS domain configuration of one or more storage virtual machines (SVMs) in your cluster to verify that it is configured properly.

Step

Viewing the DNS domain configurations by using the vserver services name-service dns show command.

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
                                         Name
                                         Servers
Vserver      State    Domains
-----
cluster-1    enabled   xyz.company.com    192.56.0.129,
                                         192.56.0.130
vs1          enabled   xyz.company.com    192.56.0.129,
                                         192.56.0.130
vs2          enabled   xyz.company.com    192.56.0.129,
                                         192.56.0.130
vs3          enabled   xyz.company.com    192.56.0.129,
                                         192.56.0.130
```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1
  Vserver: vs1
  Domains: xyz.company.com
  Name Servers: 192.56.0.129, 192.56.0.130
  Enable/Disable DNS: enabled
  Timeout (secs): 2
  Maximum Attempts: 1
```

View ONTAP failover group information

You can view information about failover groups, including the list of nodes and ports in each failover group, whether failover is enabled or disabled, and the type of failover policy that is being applied to each LIF.

Steps

1. Display the target ports for each failover group by using the `network interface failover-groups show` command.

The following command displays information about all failover groups on a two-node cluster:

```
network interface failover-groups show
  Failover
  Vserver      Group      Targets
  -----
  Cluster
    Cluster
      cluster1-01:e0a, cluster1-01:e0b,
      cluster1-02:e0a, cluster1-02:e0b
  vs1
    Default
      cluster1-01:e0c, cluster1-01:e0d,
      cluster1-01:e0e, cluster1-02:e0c,
      cluster1-02:e0d, cluster1-02:e0e
```

Learn more about `network interface failover-groups show` in the [ONTAP command reference](#).

2. Display the target ports and broadcast domain for a specific failover group by using the `network interface failover-groups show` command.

The following command displays detailed information about failover group data12 for SVM vs4:

```

network interface failover-groups show -vserver vs4 -failover-group
data12

    Vserver Name: vs4
    Failover Group Name: data12
    Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                      cluster1-02:e0g
    Broadcast Domain: Default

```

3. Display the failover settings used by all LIFs by using the `network interface show` command.

The following command displays the failover policy and failover group that is being used by each LIF:

network interface show -vserver * -lif * -fields failover-group, failover-policy			
vserver	lif	failover-policy	failover-group
Cluster	cluster1-01_clus_1	local-only	Cluster
Cluster	cluster1-01_clus_2	local-only	Cluster
Cluster	cluster1-02_clus_1	local-only	Cluster
Cluster	cluster1-02_clus_2	local-only	Cluster
cluster1	cluster_mgmt	broadcast-domain-wide	Default
cluster1	cluster1-01_mgmt1	local-only	Default
cluster1	cluster1-02_mgmt1	local-only	Default
vs1	data1	disabled	Default
vs3	data2	system-defined	group2

Learn more about `network interface show` in the [ONTAP command reference](#).

View ONTAP LIF failover targets

You might have to check whether the failover policies and the failover groups of a LIF are configured correctly. To prevent misconfiguration of the failover rules, you can display the failover targets for a single LIF or for all LIFs.

About this task

Displaying LIF failover targets enables you to check for the following:

- Whether the LIFs are configured with the correct failover group and failover policy
- Whether the resulting list of failover target ports is appropriate for each LIF
- Whether the failover target of a data LIF is not a management port (e0M)

Step

Display the failover targets of a LIF by using the `failover` option of the `network interface show`

command.

The following command displays information about the failover targets for all LIFs in a two-node cluster. The Failover Targets row shows the (prioritized) list of node-port combinations for a given LIF.

```
network interface show -failover
  Logical          Home          Failover          Failover
Vserver  Interface    Node:Port    Policy        Group
-----  -----
Cluster
  node1_clus1    node1:e0a      local-only      Cluster
  Failover Targets: node1:e0a,
                    node1:e0b
  node1_clus2    node1:e0b      local-only      Cluster
  Failover Targets: node1:e0b,
                    node1:e0a
  node2_clus1    node2:e0a      local-only      Cluster
  Failover Targets: node2:e0a,
                    node2:e0b
  node2_clus2    node2:e0b      local-only      Cluster
  Failover Targets: node2:e0b,
                    node2:e0a
cluster1
  cluster_mgmt    node1:e0c      broadcast-domain-wide
                                Default
  Failover Targets: node1:e0c,
                    node1:e0d,
                    node2:e0c,
                    node2:e0d
  node1_mgmt1    node1:e0c      local-only      Default
  Failover Targets: node1:e0c,
                    node1:e0d
  node2_mgmt1    node2:e0c      local-only      Default
  Failover Targets: node2:e0c,
                    node2:e0d
vs1
  data1          node1:e0e      system-defined  bcast1
  Failover Targets: node1:e0e,
                    node1:e0f,
                    node2:e0e,
                    node2:e0f
```

Learn more about `network interface show` in the [ONTAP command reference](#).

View ONTAP LIFs in a load balancing zone

You can verify whether a load balancing zone is configured correctly by displaying all of the LIFs that belong to it. You can also view the load balancing zone of a particular LIF, or the load balancing zones for all LIFs.

Step

Display the LIFs and load balancing details that you want by using one of the following commands

To display...	Enter...
LIFs in a particular load balancing zone	<code>network interface show -dns-zone zone_name</code> <code>zone_name</code> specifies the name of the load balancing zone.
The load balancing zone of a particular LIF	<code>network interface show -lif lif_name -fields dns-zone</code>
The load balancing zones of all LIFs	<code>network interface show -fields dns-zone</code>

Examples of displaying load balancing zones for LIFs

The following command displays the details of all LIFs in the load balancing zone `storage.company.com` for SVM `vs0`:

```
net int show -vserver vs0 -dns-zone storage.company.com

      Logical      Status      Network          Current      Current  Is
Vserver  Interface  Admin/Oper Address/Mask  Node        Port    Home
-----  -----  -----  -----  -----  -----  -----  -----
vs0
      lif3      up/up    10.98.226.225/20  ndeux-11  e0c    true
      lif4      up/up    10.98.224.23/20   ndeux-21  e0c    true
      lif5      up/up    10.98.239.65/20  ndeux-11  e0c    true
      lif6      up/up    10.98.239.66/20  ndeux-11  e0c    true
      lif7      up/up    10.98.239.63/20  ndeux-21  e0c    true
      lif8      up/up    10.98.239.64/20  ndeux-21  e0c    true
```

The following command displays the DNS zone details of the LIF `data3`:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif      dns-zone
-----  -----  -----
vs0      data3    storage.company.com
```

The following command displays the list of all LIFs in the cluster and their corresponding DNS zones:

```
network interface show -fields dns-zone
Vserver    lif          dns-zone
-----
cluster    cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0        data1        storage.company.com
vs0        data2        storage.company.com
```

Learn more about `network interface show` in the [ONTAP command reference](#).

View ONTAP cluster connections

You can display all the active connections in the cluster or a count of active connections on the node by client, logical interface, protocol, or service. You can also display all the listening connections in the cluster.

Display active connections by client (cluster administrators only)

You can view the active connections by client to verify the node that a specific client is using and to view possible imbalances between client counts per node.

About this task

The count of active connections by client is useful in the following scenarios:

- Finding a busy or overloaded node.
- Determining why a particular client's access to a volume is slow.

You can view details about the node that the client is accessing and then compare it with the node on which the volume resides. If accessing the volume requires traversing the cluster network, clients might experience decreased performance because of the remote access to the volume on an oversubscribed remote node.

- Verifying that all nodes are being used equally for data access.
- Finding clients that have an unexpectedly high number of connections.
- Verifying whether certain clients have connections to a node.

Step

Display a count of the active connections by client on a node by using the `network connections active show-clients` command.

Learn more about `network connections active show-clients` in the [ONTAP command reference](#).

network connections active show-clients			
Node	Vserver Name	Client IP Address	Count
node0	vs0	192.0.2.253	1
	vs0	192.0.2.252	2
	Cluster	192.10.2.124	5
node1	vs0	192.0.2.250	1
	vs0	192.0.2.252	3
	Cluster	192.10.2.123	4
node2	vs1	customer.example.com	1
	vs1	192.0.2.245	3
	Cluster	192.10.2.122	4
node3	vs1	customer.example.org	1
	vs1	customer.example.net	3
	Cluster	192.10.2.121	4

Display active connections by protocol (cluster administrators only)

You can display a count of the active connections by protocol (TCP or UDP) on a node to compare the usage of protocols within the cluster.

About this task

The count of active connections by protocol is useful in the following scenarios:

- Finding the UDP clients that are losing their connection.

If a node is near its connection limit, UDP clients are the first to be dropped.

- Verifying that no other protocols are being used.

Step

Display a count of the active connections by protocol on a node by using the `network connections active show-protocols` command.

Learn more about `network connections active show-protocols` in the [ONTAP command reference](#).

```
network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----  -----  -----  -----
node0
    vs0          UDP      19
    Cluster      TCP      11
node1
    vs0          UDP      17
    Cluster      TCP      8
node2
    vs1          UDP      14
    Cluster      TCP      10
node3
    vs1          UDP      18
    Cluster      TCP      4
```

Display active connections by service (cluster administrators only)

You can display a count of the active connections by service type (for example, by NFS, SMB, mount, and so on) for each node in a cluster. This is useful to compare the usage of services within the cluster, which helps to determine the primary workload of a node.

About this task

The count of active connections by service is useful in the following scenarios:

- Verifying that all nodes are being used for the appropriate services and that the load balancing for that service is working.
- Verifying that no other services are being used. Display a count of the active connections by service on a node by using the `network connections active show-services` command.

Learn more about `network connections active show-services` in the [ONTAP command reference](#).

network connections active show-services			
Node	Vserver Name	Service	Count
node0			
	vs0	mount	3
	vs0	nfs	14
	vs0	nlm_v4	4
	vs0	cifs_srv	3
	vs0	port_map	18
	vs0	rclopcp	27
	Cluster	ctlopcp	60
node1			
	vs0	cifs_srv	3
	vs0	rclopcp	16
	Cluster	ctlopcp	60
node2			
	vs1	rclopcp	13
	Cluster	ctlopcp	60
node3			
	vs1	cifs_srv	1
	vs1	rclopcp	17
	Cluster	ctlopcp	60

Display active connections by LIF on a node and SVM

You can display a count of active connections for each LIF, by node and storage virtual machine (SVM), to view connection imbalances between LIFs within the cluster.

About this task

The count of active connections by LIF is useful in the following scenarios:

- Finding an overloaded LIF by comparing the number of connections on each LIF.
- Verifying that DNS load balancing is working for all data LIFs.
- Comparing the number of connections to the various SVMs to find the SVMs that are used the most.

Step

Display a count of active connections for each LIF by SVM and node by using the `network connections active show-lifs` command.

Learn more about `network connections active show-lifs` in the [ONTAP command reference](#).

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----  -----  -----  -----
node0
    vs0          datalif1          3
    Cluster      node0_clus_1      6
    Cluster      node0_clus_2      5
node1
    vs0          datalif2          3
    Cluster      node1_clus_1      3
    Cluster      node1_clus_2      5
node2
    vs1          datalif2          1
    Cluster      node2_clus_1      5
    Cluster      node2_clus_2      3
node3
    vs1          datalif1          1
    Cluster      node3_clus_1      2
    Cluster      node3_clus_2      2

```

Display active connections in a cluster

You can display information about the active connections in a cluster to view the LIF, port, remote host, service, storage virtual machines (SVMs), and protocol used by individual connections.

About this task

Viewing the active connections in a cluster is useful in the following scenarios:

- Verifying that individual clients are using the correct protocol and service on the correct node.
- If a client is having trouble accessing data using a certain combination of node, protocol, and service, you can use this command to find a similar client for configuration or packet trace comparison.

Step

Display the active connections in a cluster by using the `network connections active show` command.

Learn more about `network connections active show` in the [ONTAP command reference](#).

The following command shows the active connections on the node node1:

```

network connections active show -node node1
Vserver  Interface          Remote
Name     Name:Local Port    Host:Port      Protocol/Service
-----
Node: node1
Cluster  node1_clus_1:50297 192.0.2.253:7700  TCP/ctlopcp
Cluster  node1_clus_1:13387 192.0.2.253:7700  TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700  TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700  TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700  TCP/ctlopcp
vs1      data1:111          host1.aa.com:10741  UDP/port-map
vs3      data2:111          host1.aa.com:10741  UDP/port-map
vs1      data1:111          host1.aa.com:12017  UDP/port-map
vs3      data2:111          host1.aa.com:12017  UDP/port-map

```

The following command shows the active connections on SVM vs1:

```

network connections active show -vserver vs1
Vserver  Interface          Remote
Name     Name:Local Port    Host:Port      Protocol/Service
-----
Node: node1
vs1      data1:111          host1.aa.com:10741  UDP/port-map
vs1      data1:111          host1.aa.com:12017  UDP/port-map

```

Display listening connections in a cluster

You can display information about the listening connections in a cluster to view the LIFs and ports that are accepting connections for a given protocol and service.

About this task

Viewing the listening connections in a cluster is useful in the following scenarios:

- Verifying that the desired protocol or service is listening on a LIF if client connections to that LIF fail consistently.
- Verifying that a UDP/rlclopccp listener is opened at each cluster LIF if remote data access to a volume on one node through a LIF on another node fails.
- Verifying that a UDP/rlclopccp listener is opened at each cluster LIF if SnapMirror transfers between two nodes in the same cluster fail.
- Verifying that a TCP/ctlopcp listener is opened at each intercluster LIF if SnapMirror transfers between two nodes in different clusters fail.

Step

Display the listening connections per node by using the `network connections listening show` command.

network connections listening show		
Vserver Name	Interface Name:Local Port	Protocol/Service
Node: node0		
Cluster	node0_clus_1:7700	TCP/ctlopcp
vs1	data1:4049	UDP/unknown
vs1	data1:111	TCP/port-map
vs1	data1:111	UDP/port-map
vs1	data1:4046	TCP/sm
vs1	data1:4046	UDP/sm
vs1	data1:4045	TCP/nlm-v4
vs1	data1:4045	UDP/nlm-v4
vs1	data1:2049	TCP/nfs
vs1	data1:2049	UDP/nfs
vs1	data1:635	TCP/mount
vs1	data1:635	UDP/mount
Cluster	node0_clus_2:7700	TCP/ctlopcp

Learn more about network connections listening show in the [ONTAP command reference](#).

ONTAP commands to diagnose network problems

You can diagnose problems on your network by using commands such as `ping`, `traceroute`, `ndp`, and `tcpdump`. You can also use commands such as `ping6` and `traceroute6` to diagnose IPv6 problems.

If you want to...	Enter this command...
Test whether the node can reach other hosts on your network	<code>network ping</code>
Test whether the node can reach other hosts on your IPv6 network	<code>network ping6</code>
Trace the route that the IPv4 packets take to a network node	<code>network traceroute</code>
Trace the route that the IPv6 packets take to a network node	<code>network traceroute6</code>
Manage the Neighbor Discovery Protocol (NDP)	<code>network ndp</code>
Display statistics about packets that are received and sent on a specified network interface or on all network interfaces	<code>run -node node_name ifstat</code> Note: This command is available from the nodeshell.
Display information about neighboring devices that are discovered from each node and port in the cluster, including the remote device type and device platform	<code>network device-discovery show</code>

View the CDP neighbors of the node (ONTAP supports only CDPv1 advertisements)	<pre>run -node <i>node_name</i> cdpd show-neighbors</pre> <p>Note: This command is available from the nodeshell.</p>
Trace the packets that are sent and received in the network	<pre>network tcpdump start -node <i>node-name</i> -port <i>port_name</i></pre> <p>Note: This command is available from the nodeshell.</p>
Measure latency and throughput between intercluster or intracluster nodes	<pre>network test -path -source-node <i>source_nodename</i> <i>local</i> -destination -cluster <i>destination_clusternode</i> -destination-node <i>destination_nodename</i> -session-type <i>Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</i></pre> <p>For more information, see the Performance management.</p>

Related information

- [ONTAP command reference](#)
- [network ping](#)
- [network traceroute](#)
- [network device-discovery show](#)
- [network ndp](#)

View network connectivity with neighbor discovery protocols

View ONTAP network connectivity with neighbor discovery protocols

In a data center, you can use neighbor discovery protocols to view network connectivity between a pair of physical or virtual systems and their network interfaces. ONTAP supports two neighbor discovery protocols: Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

Neighbor discovery protocols enable you to automatically discover and view information about directly connected protocol-enabled devices in a network. Each device advertises identification, capabilities, and connectivity information. This information is transmitted in Ethernet frames to a multicast MAC address and is received by all neighboring protocol-enabled devices.

For two devices to become neighbors, each must have a protocol enabled and correctly configured. Discovery protocol functionality is limited to directly connected networks. Neighbors can include protocol-enabled devices such as switches, routers, bridges, and so on. ONTAP supports two neighbor discovery protocols, which can be used individually or together.

Cisco Discovery Protocol (CDP)

CDP is a proprietary link layer protocol developed by Cisco Systems. It is enabled by default in ONTAP for

cluster ports, but must be enabled explicitly for data ports.

Link Layer Discovery Protocol (LLDP)

LLDP is a vendor-neutral protocol specified in the standards document IEEE 802.1AB. It must be enabled explicitly for all ports.

Use CDP to detect ONTAP network connectivity

Using CDP to detect network connectivity consists of reviewing deployment considerations, enabling it on data ports, viewing neighbor devices, and adjusting CDP configuration values as needed. CDP is enabled by default on cluster ports.

CDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP release	Description
9.10.1 and earlier	CDP is also used by the cluster switch health monitor to automatically discover your cluster and management network switches.
9.11.1 and later	CDP is also used by the cluster switch health monitor to automatically discover your cluster, storage, and management network switches.

Related information

[System administration](#)

Considerations for using CDP

By default, CDP-compliant devices send CDPv2 advertisements. CDP-compliant devices send CDPv1 advertisements only when they receive CDPv1 advertisements. ONTAP supports only CDPv1. Therefore, when an ONTAP node sends CDPv1 advertisements, CDP-compliant neighboring devices send back CDPv1 advertisements.

You should consider the following information before enabling CDP on a node:

- CDP is supported for all ports.
- CDP advertisements are sent and received by ports that are in the up state.
- CDP must be enabled on both the transmitting and receiving devices for sending and receiving CDP advertisements.
- CDP advertisements are sent at regular intervals, and you can configure the time interval.
- When IP addresses are changed for a LIF, the node sends the updated information in the next CDP advertisement.
- ONTAP 9.10.1 and earlier:
 - CDP is always enabled on cluster ports.
 - CDP is disabled, by default, on all non-cluster ports.
- ONTAP 9.11.1 and later:
 - CDP is always enabled on cluster and storage ports.

- CDP is disabled, by default, on all non-cluster and non-storage ports.



Sometimes when LIFs are changed on the node, the CDP information is not updated at the receiving device side (for example, a switch). If you encounter such a problem, you should configure the network interface of the node to the down status and then to the up status.

- Only IPv4 addresses are advertised in CDP advertisements.
- For physical network ports with VLANs, all of the LIFs configured on the VLANs on that port are advertised.
- For physical ports that are part of an interface group, all of the IP addresses configured on that interface group are advertised on each physical port.
- For an interface group that hosts VLANs, all of the LIFs configured on the interface group and the VLANs are advertised on each of the network ports.
- Due to CDP packets being restricted to no more than 1500 bytes, on ports configured with a large number of LIFs only a subset of these IP addresses may be reported on the adjacent switch.

Enable or disable CDP

To discover and send advertisements to CDP-compliant neighboring devices, CDP must be enabled on each node of the cluster.

By default in ONTAP 9.10.1 and earlier, CDP is enabled on all cluster ports of a node and disabled on all non-cluster ports of a node.

By default in ONTAP 9.11.1 and later, CDP is enabled on all cluster and storage ports of a node and disabled on all non-cluster and non-storage ports of a node.

About this task

The `cdpd.enable` option controls whether CDP is enabled or disabled on the ports of a node:

- For ONTAP 9.10.1 and earlier, on enables CDP on non-cluster ports.
- For ONTAP 9.11.1 and later, on enables CDP on non-cluster and non-storage ports.
- For ONTAP 9.10.1 and earlier, off disables CDP on non-cluster ports; you cannot disable CDP on cluster ports.
- For ONTAP 9.11.1 and later, off disables CDP on non-cluster and non-storage ports; you cannot disable CDP on cluster ports.

When CDP is disabled on a port that is connected to a CDP-compliant device, network traffic might not be optimized.

Steps

1. Display the current CDP setting for a node, or for all nodes in a cluster:

To view the CDP setting of...	Enter...
A node	<code>run - node <node_name> options cdpd.enable</code>
All nodes in a cluster	<code>options cdpd.enable</code>

2. Enable or disable CDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable CDP on...	Enter...
A node	run -node node_name options cdpd.enable {on or off}
All nodes in a cluster	options cdpd.enable {on or off}

View CDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to a CDP-compliant device. You can use the `network device-discovery show -protocol cdp` command to view neighbor information. Learn more about `network device-discovery show` in the [ONTAP command reference](#).

About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for cluster ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster ports for neighbor information to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster and non-storage ports for neighbor information to appear for those ports.

Step

Display information about all CDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol cdp
```

The following command shows the neighbors that are connected to the ports on node sti2650-212:

```

network device-discovery show -node sti2650-212 -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface      Platform
-----
-----
sti2650-212/cdp
      e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                           Ethernet1/14      N9K-
C93120TX
      e0a    CS:RTP-CS01-510K35      0/8      CN1610
      e0b    CS:RTP-CS01-510K36      0/8      CN1610
      e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                           Ethernet1/21      N9K-
C93180YC-FX
      e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/22      N9K-
C93180YC-FX
      e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/23      N9K-
C93180YC-FX
      e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/24      N9K-
C93180YC-FX

```

The output lists the Cisco devices that are connected to each port of the specified node.

Configure the hold time for CDP messages

Hold time is the period of time for which CDP advertisements are stored in cache in neighboring CDP-compliant devices. Hold time is advertised in each CDPv1 packet and is updated whenever a CDPv1 packet is received by a node.

- The value of the `cdpd.holddate` option should be set to the same value on both nodes of an HA pair.
- The default hold time value is 180 seconds, but you can enter values ranging from 10 seconds to 255 seconds.
- If an IP address is removed before the hold time expires, the CDP information is cached until the hold time expires.

Steps

1. Display the current CDP hold time for a node, or for all nodes in a cluster:

To view the hold time of...	Enter...
A node	<code>run -node node_name options cdpd.holddate</code>
All nodes in a cluster	<code>options cdpd.holddate</code>

2. Configure the CDP hold time on all ports of a node, or on all ports of all nodes in a cluster:

To set the hold time on...	Enter...
A node	run -node node_name options cdpd.holddate holddate
All nodes in a cluster	options cdpd.holddate holddate

Set the interval for sending CDP advertisements

CDP advertisements are sent to CDP neighbors at periodic intervals. You can increase or decrease the interval for sending CDP advertisements depending on network traffic and changes in the network topology.

- The value of the `cdpd.interval` option should be set to the same value on both nodes of an HA pair.
- The default interval is 60 seconds, but you can enter a value from 5 seconds to 900 seconds.

Steps

1. Display the current CDP advertisement time interval for a node, or for all nodes in a cluster:

To view the interval for...	Enter...
A node	run -node node_name options cdpd.interval
All nodes in a cluster	options cdpd.interval

2. Configure the interval for sending CDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

To set the interval for...	Enter...
A node	run -node node_name options cdpd.interval interval
All nodes in a cluster	options cdpd.interval interval

View or clear CDP statistics

You can view the CDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. CDP statistics are cumulative from the time they were last cleared.

About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on ports for statistics to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on non-cluster or non-storage ports for statistics to appear for those ports.

Step

Display or clear the current CDP statistics for all ports on a node:

If you want to...	Enter...
View the CDP statistics	run -node node_name cdpd show-stats
Clear the CDP statistics	run -node node_name cdpd zero-stats

Example of showing and clearing statistics

The following command shows the CDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
run -node node1 cdpd show-stats

RECEIVE
  Packets: 9116 | Csum Errors: 0 | Unsupported Vers: 4561
  Invalid length: 0 | Malformed: 0 | Mem alloc fails: 0
  Missing TLVs: 0 | Cache overflow: 0 | Other errors: 0

TRANSMIT
  Packets: 4557 | Xmit fails: 0 | No hostname: 0
  Packet truncated: 0 | Mem alloc fails: 0 | Other errors: 0

OTHER
  Init failures: 0
```

The following command clears the CDP statistics:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
  Packets: 0 | Csum Errors: 0 | Unsupported Vers: 0
  Invalid length: 0 | Malformed: 0 | Mem alloc fails: 0
  Missing TLVs: 0 | Cache overflow: 0 | Other errors: 0

TRANSMIT
  Packets: 0 | Xmit fails: 0 | No hostname: 0
  Packet truncated: 0 | Mem alloc fails: 0 | Other errors: 0

OTHER
  Init failures: 0
```

After the statistics are cleared, they begin to accumulate after the next CDP advertisement is sent or received.

Connecting to Ethernet switches that do not support CDP

Several vendor switches do not support CDP. See the [NetApp Knowledge Base: ONTAP device discovery shows nodes instead of the switch](#) for further details.

There are two options to resolve this issue:

- Disable CDP and enable LLDP, if supported. See [Use LLDP to detect network connectivity](#) for further details.
- Configure a MAC address packet filter on the switches to drop CDP advertisements.

Use LLDP to detect ONTAP network connectivity

Using LLDP to detect network connectivity consists of reviewing deployment considerations, enabling it on all ports, viewing neighbor devices, and adjusting LLDP configuration values as needed.

LLDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP currently reports the following type-length-value structures (TLVs):

- Chassis ID
- Port ID
- Time-To-Live (TTL)
- System name

The system name TLV is not sent on CNA devices.

Certain converged network adapters (CNAs), such as the X1143 adapter and the UTA2 onboard ports, contain offload support for LLDP:

- LLDP offload is used for Data Center Bridging (DCB).
- Displayed information might differ between the cluster and the switch.

The Chassis ID and Port ID data displayed by the switch might be different for CNA and non-CNA ports.

For example:

- For non-CNA ports:
 - Chassis ID is a fixed MAC address of one of the ports on the node
 - Port ID is the port name of the respective port on the node
- For CNA ports:
 - Chassis ID and Port ID are the MAC addresses of the respective ports on the node.

However, the data displayed by the cluster is consistent for these port types.



The LLDP specification defines access to the collected information through an SNMP MIB. However, ONTAP does not currently support the LLDP MIB.

Enable or disable LLDP

To discover and send advertisements to LLDP-compliant neighboring devices, LLDP must be enabled on each node of the cluster. Beginning with ONTAP 9.7, LLDP is enabled on all ports of a node by default.

About this task

For ONTAP 9.10.1 and earlier, the `lldp.enable` option controls whether LLDP is enabled or disabled on the ports of a node:

- `on` enables LLDP on all ports.
- `off` disables LLDP on all ports.

For ONTAP 9.11.1 and later, the `lldp.enable` option controls whether LLDP is enabled or disabled on the non-cluster and non-storage ports of a node:

- `on` enables LLDP on all non-cluster and non-storage ports.
- `off` disables LLDP on all non-cluster and non-storage ports.

Steps

1. Display the current LLDP setting for a node, or for all nodes in a cluster:

- Single node: `run -node node_name options lldp.enable`
- All nodes: `options lldp.enable`

2. Enable or disable LLDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable LLDP on...	Enter...
A node	<code>run -node node_name options lldp.enable {on off}</code>
All nodes in a cluster	<code>options lldp.enable {on off}</code>

- Single node:

```
run -node node_name options lldp.enable {on|off}
```

- All nodes:

```
options lldp.enable {on|off}
```

View LLDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to an LLDP-compliant device. You use the network device-discovery show command to view neighbor information.

Step

1. Display information about all LLDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol lldp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01. The output lists the LLDP-enabled devices that are connected to each port of the specified node. If the -protocol option is omitted, the output also lists CDP-enabled devices.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/      Local   Discovered
Protocol   Port    Device           Interface      Platform
-----  -----  -----
-----  -----
cluster-1_01/lldp
      e2a    0013.c31e.5c60      GigabitEthernet1/36
      e2b    0013.c31e.5c60      GigabitEthernet1/35
      e2c    0013.c31e.5c60      GigabitEthernet1/34
      e2d    0013.c31e.5c60      GigabitEthernet1/33
```

Adjust the interval for transmitting LLDP advertisements

LLDP advertisements are sent to LLDP neighbors at periodic intervals. You can increase or decrease the interval for sending LLDP advertisements depending on network traffic and changes in the network topology.

About this task

The default interval recommended by IEEE is 30 seconds, but you can enter a value from 5 seconds to 300 seconds.

Steps

1. Display the current LLDP advertisement time interval for a node, or for all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.interval
```

- All nodes:

```
options lldp.xmit.interval
```

2. Adjust the interval for sending LLDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- All nodes:

```
options lldp.xmit.interval <interval>
```

Adjust the time-to-live value for LLDP advertisements

Time-To-Live (TTL) is the period of time for which LLDP advertisements are stored in cache in neighboring LLDP-compliant devices. TTL is advertised in each LLDP packet and is updated whenever an LLDP packet is received by a node. TTL can be modified in outgoing LLDP frames.

About this task

- TTL is a calculated value, the product of the transmit interval (`lldp.xmit.interval`) and the hold multiplier (`lldp.xmit.hold`) plus one.
- The default hold multiplier value is 4, but you can enter values ranging from 1 to 100.
- The default TTL is therefore 121 seconds, as recommended by IEEE, but by adjusting the transmit interval and hold multiplier values, you can specify a value for outgoing frames from 6 seconds to 30001 seconds.
- If an IP address is removed before the TTL expires, the LLDP information is cached until the TTL expires.

Steps

1. Display the current hold multiplier value for a node, or for all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold
```

- All nodes:

```
options lldp.xmit.hold
```

2. Adjust the hold multiplier value on all ports of a node, or on all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- All nodes:

```
options lldp.xmit.hold <hold_value>
```

View or clear LLDP statistics

You can view the LLDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. LLDP statistics are cumulative from the time they were last cleared.

About this task

For ONTAP 9.10.1 and earlier, because LLDP is always enabled for cluster ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster ports for statistics to appear for those ports.

For ONTAP 9.11.1 and later, because LLDP is always enabled for cluster and storage ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster and non-storage ports for statistics to appear for those ports.

Step

Display or clear the current LLDP statistics for all ports on a node:

If you want to...	Enter...
View the LLDP statistics	run -node node_name lldp stats
Clear the LLDP statistics	run -node node_name lldp stats -z

Show and clear statistics example

The following command shows the LLDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
  Total frames:      190k | Accepted frames:      190k | Total drops:
  0
TRANSMIT
  Total frames:      5195 | Total failures:          0
OTHER
  Stored entries:      64
```

The following command clears the LLDP statistics.

```
cluster-1::> The following command clears the LLDP statistics:  
run -node vsim1 lldp stats -z  
run -node node1 lldp stats
```

RECEIVE

Total frames:	0		Accepted frames:	0		Total drops:	0
---------------	---	--	------------------	---	--	--------------	---

TRANSMIT

Total frames:	0		Total failures:	0
---------------	---	--	-----------------	---

OTHER

Stored entries:	64
-----------------	----

After the statistics are cleared, they begin to accumulate after the next LLDP advertisement is sent or received.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.